

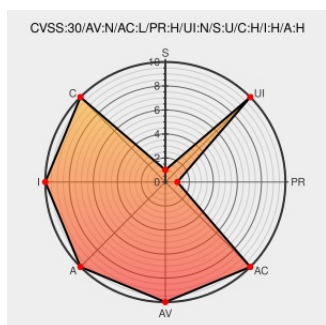


CVE-2020-2798

Published on: 04/15/2020 12:00:00 AM UTC

Last Modified on: 10/14/2022 06:09:00 PM UTC

CVE-2020-2798

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Weblogic Server](#) from [Oracle](#) contain the following vulnerability:

Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: WLS Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows high privileged attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server.

Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.

CVSS 3.0 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).

CVE-2020-2798 has been assigned by [secalert_us@oracle.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Oracle Corporation](#) - **WebLogic Server** version = **10.3.6.0.0**

Affected Vendor/Software: [Oracle Corporation](#) - **WebLogic Server** version = **12.1.3.0.0**

Affected Vendor/Software: [Oracle Corporation](#) - **WebLogic Server** version = **12.2.1.3.0**

Affected Vendor/Software: [Oracle Corporation](#) - **WebLogic Server** version = **12.2.1.4.0**

CVSS3 Score: **7.2 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Oracle Critical Patch Update Advisory - April 2020	Vendor Advisory www.oracle.com text/html	MISC www.oracle.com/security-alerts/cpuapr2020.html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

CVE-2020-2546 , CVE-2020-2915 CVE-2020-2801 CVE-2020-2798 CVE-2020-2883 CVE-2020-2884 CVE-2020-2950 WebLogic T3 payload...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Weblogic Server	10.3.6.0.0	All	All	All
Application	Oracle	Weblogic Server	12.1.3.0.0	All	All	All
Application	Oracle	Weblogic Server	12.2.1.3.0	All	All	All
Application	Oracle	Weblogic Server	12.2.1.4.0	All	All	All
Application	Oracle	Weblogic Server	10.3.6.0.0	All	All	All
Application	Oracle	Weblogic Server	12.1.3.0.0	All	All	All
Application	Oracle	Weblogic Server	12.2.1.3.0	All	All	All
Application	Oracle	Weblogic Server	12.2.1.4.0	All	All	All

```
cpe:2.3:a:oracle:weblogic_server:10.3.6.0.0:*:*:*:*:*:*
```

```
cpe:2.3:a:oracle:weblogic server:12.1.3.0.0:*:*:*:*:*:*
```

```
cpe:2.3:a:oracle:weblogic server:12.2.1.3.0:::*:*:*:*:*
```

```
cpe:2.3:a:oracle:weblogic server:12.2.1.4.0:::*:*:*:*:*
```

```
cpe:2.3:a:oracle:weblogic server:10.3.6.0.0:*:*:*:*:*:*
```

```
cpe:2.3:a:oracle:weblogic server:12.1.3.0.0:*:*:*:*:*:*
```

```
one:2 3:2 oracle:weblogic server:12 2 1 3 0.*.*.*.*.*.*.*.*.*.*
```

```
cpe:2.3:a:oracle:weblogic_server:12.2.1.4.0:::*:*:*:*:*:
```

Social Mentions

Next ID→

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE.report and Source URL Uptime Status status.cve.report